Configurar SCA para Ingerir Várias Contas AWS através de um Único Recipiente AWS S3

Contents

Introduction

Este documento descreve como você configura um Amazon Web Services (AWS) Simple Storage Service (S3) para aceitar logs de uma segunda conta AWS.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Análise de nuvem segura
- Gerenciamento de acesso de identidade (IAM) do AWS
- AWS S3

Componentes Utilizados

As informações neste documento são baseadas em:

- AWS Conta A (referida como ACCOUNT_A_ID - Esta conta hospeda/possui os buckets S3 que já existem)
- AWS Conta B (conhecida como ACCOUNT_B_ID - Esta é uma nova conta (para Secure

Cloud Analytics) que envia dados para S3_BUCKET_NAME da ACCOUNT_A_ID)
- Secure Cloud Analytics (isso já deve estar integrado com ACCOUNT_A_ID)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Há cinco etapas para que o SCA receba contas 2+ de um depósito S3:

1. Atualizar **ACCOUNT_A_ID's S3_BUCKET_NAME** política de concessão **ACCOUNT_B_ID** permissões de gravação da conta.
2. Configurar o **ACCOUNT_B_ID** conta para a qual enviar Logs de Fluxo VPC **ACCOUNT_A_ID's S3_BUCKET_NAME**.
3. Criar política IAM em **ACCOUNT_B_ID's** Painel do AWS IAM.
4. Criar função IAM em **ACCOUNT_B_ID's** Painel do AWS IAM.
5. Configurar Credenciais de Análise de Nuvem Segura para **ACCOUNT_B_ID**.

Diagrama de Rede

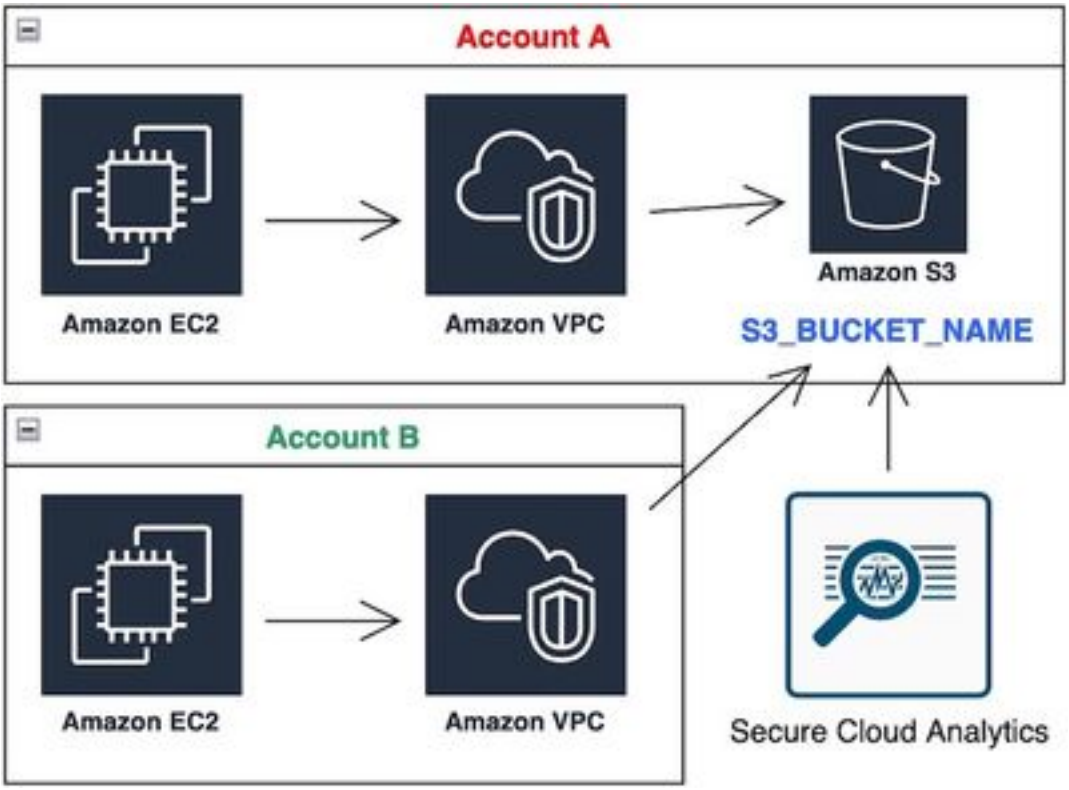


Diagrama de Fluxo de Dados

Configurações

1. Atualize a Política S3_BUCKET_NAME da ACCOUNT_A_ID para Conceder Permissões de Gravação de Conta ACCOUNT_B_ID

ACCOUNT_A_ID's S3_BUCKET_NAME a configuração da política de bucket é fornecida aqui. Essa configuração permite que uma conta secundária (ou qualquer número de contas desejado) grave (SID-AWSLogDeliveryWrite) no bucket de S3 e verifique as ACLs (SID -

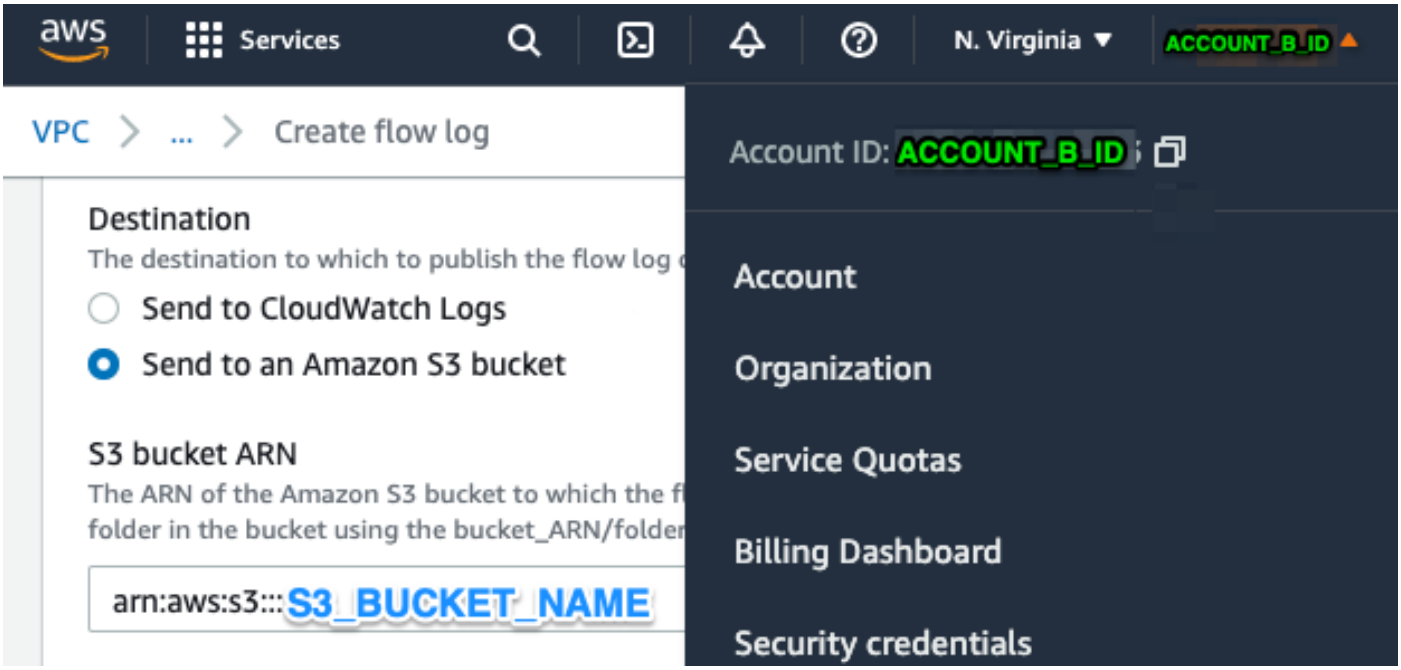
AWSLogDeliveryAclCheck) do bucket.

- alteram **ACCOUNT_A_ID** e **ACCOUNT_B_ID** a seus respectivos valores numéricos sem traços.
- alteram **S3_BUCKET_NAME** para o respectivo nome do bucket.
- Ignore a formatação aqui. O AWS pode editá-la conforme necessário.

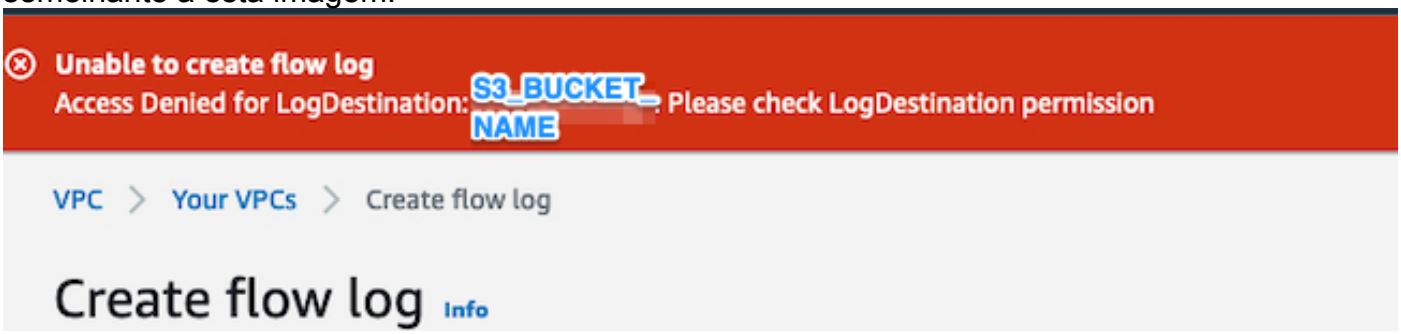
```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AWSLogDeliveryWrite",
"Effect": "Allow",
"Principal": {"Service": "delivery.logs.amazonaws.com"},
"Action": "s3:PutObject",
"Resource": ["arn:aws:s3:::S3_BUCKET_NAME","arn:aws:s3:::S3_BUCKET_NAME/*"],
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"ArnLike": {"aws:SourceArn": ["arn:aws:logs:*:ACCOUNT_A_ID:*","arn:aws:logs:*:ACCOUNT_B_ID:*"]}
}
},
{
"Sid": "AWSLogDeliveryAclCheck",
"Effect": "Allow",
"Principal": {
"Service": "delivery.logs.amazonaws.com"
},
"Action": "s3:GetBucketAcl",
"Resource": "arn:aws:s3:::S3_BUCKET_NAME",
"Condition": {
"StringEquals": {"aws:SourceAccount": ["ACCOUNT_A_ID","ACCOUNT_B_ID"]},
"ArnLike": {"aws:SourceArn": ["arn:aws:logs:*:ACCOUNT_A_ID:*","arn:aws:logs:*:ACCOUNT_B_ID:*"]}
}
}
]
}
```

2. Configure a Conta ACCOUNT_B_ID para Enviar Logs de Fluxo de VPC para S3_BUCKET_NAME de ACCOUNT_A_ID

Criar um Log de Fluxo do VPC **ACCOUNT_B_ID** que **ACCOUNT_A_ID'sS3_BUCKET_NAME** Bucket ARN no destino como mostrado nesta imagem:



Se as permissões no bucket de S3 não estiverem configuradas corretamente, você verá um erro semelhante a esta imagem:



3. Criar Política IAM no Painel do AWS IAM do ACCOUNT_B_ID

A configuração da Política IAM anexada a swc_role em ACCOUNT_B_ID é:

```
swc_single_policy
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"autoscaling:Describe*",
"cloudtrail:LookupEvents",
"cloudwatch:Get*",
"cloudwatch:List*",
"ec2:Describe*",
"ecs:List*",
"ecs:Describe*",
"elasticache:Describe*",
"elasticache:List*",
"elasticloadbalancing:Describe*",
"guardduty:Get*",
"guardduty:List*",
"iam:Get*",
"iam:List*",
"inspector:*",
```

```
"rds:Describe*",
"rds:List*",
"redshift:Describe*",
"workspaces:Describe*",
"route53:List*"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Action": [
"logs:Describe*",
"logs:GetLogEvents",
"logs:FilterLogEvents",
"logs:PutSubscriptionFilter",
"logs:DeleteSubscriptionFilter"
],
"Effect": "Allow",
"Resource": "*"
},
{
"Sid": "CloudCompliance",
"Action": [
"access-analyzer:ListAnalyzers",
"cloudtrail:DescribeTrails",
"cloudtrail:GetEventSelectors",
"cloudtrail:GetTrailStatus",
"cloudtrail:ListTags",
"cloudwatch:DescribeAlarmsForMetric",
"config:Get*",
"config:Describe*",
"ec2:GetEbsEncryptionByDefault",
"iam:GenerateCredentialReport",
"iam:Get*",
"iam:List*",
"kms:GetKeyRotationStatus",
"kms:ListKeys",
"logs:DescribeMetricFilters",
"logs:Describe*",
"logs:GetLogEvents",
"logs:FilterLogEvents",
"organizations:ListPolicies",
"s3:GetAccelerateConfiguration",
"s3:GetAccessPoint",
"s3:GetAccessPointPolicy",
"s3:GetAccessPointPolicyStatus",
"s3:GetAccountPublicAccessBlock",
"s3:GetAnalyticsConfiguration",
"s3:GetBucket*",
"s3:GetEncryptionConfiguration",
"s3:GetInventoryConfiguration",
"s3:GetLifecycleConfiguration",
"s3:GetMetricsConfiguration",
"s3:GetObjectAcl",
"s3:GetObjectVersionAcl",
"s3:GetReplicationConfiguration",
"s3:ListAccessPoints",
"s3:ListAllMyBuckets",
"securityhub:Get*",
"sns:ListSubscriptionsByTopic"
],
"Effect": "Allow",
"Resource": "*"
},
```

```
{
"Action": [
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject"
],
"Effect": "Allow",
"Resource": [
"arn:aws:s3:::S3_BUCKET_NAME/*",
"arn:aws:s3:::S3_BUCKET_NAME"
]
}
]
}
```

4. Criar Função IAM no Painel do AWS IAM do ACCOUNT_B_ID

1. Selecione **Roles**.

2. Selecione **Create role**.

3. Selecione o tipo de função Outra conta AWS.

4. Informe 757972810156 no campo ID da Conta.

5. Selecione a opção Exigir ID externa.

6. Insira o nome do portal da Web Secure Cloud Analytics como **External ID**.
7. Clique em **Next: Permissions .**

8. Selecione a opção **swc_single_policy** que você acabou de criar.

9. Clique em **Next: Tagging**.

10. Clique em **Next: Review**.

11. Informe swc_role como o nome da Função.

12. Informe um **Description**, como uma Função para permitir o acesso entre contas.

13. Clique em **Create role** .

14. Copie a função ARN e cole-a em um editor de texto simples.

5. Configurar Credenciais de Análise de Nuvem Segura para ACCOUNT_B_ID

1. Faça login no Secure Cloud Analytics e selecione **Settings > Integrations > AWS > Credentials**.

2. Clique em **Add New Credentials**.

3. Para efeitos da **Name**, o esquema de nomenclatura sugerido seria **Account_B_ID_creds** (por exemplo; 012345678901_creds) para cada conta, você deseja incluir.

4. Cole o ARN da função da etapa anterior e cole-o no **Role ARN** campo.

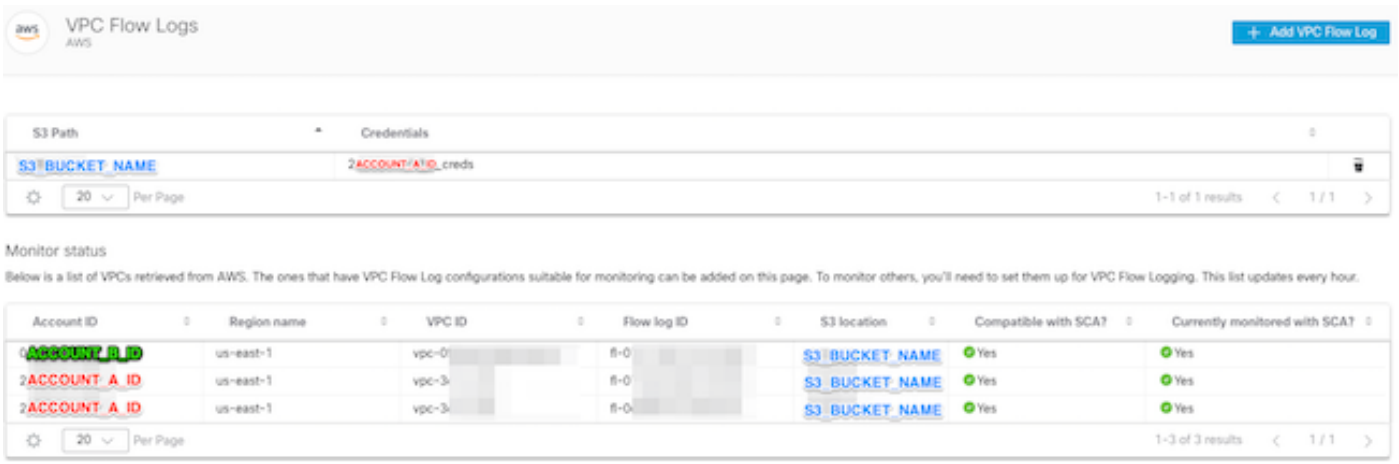
5. Clique em **Create**.

Nenhuma etapa de configuração adicional é necessária.

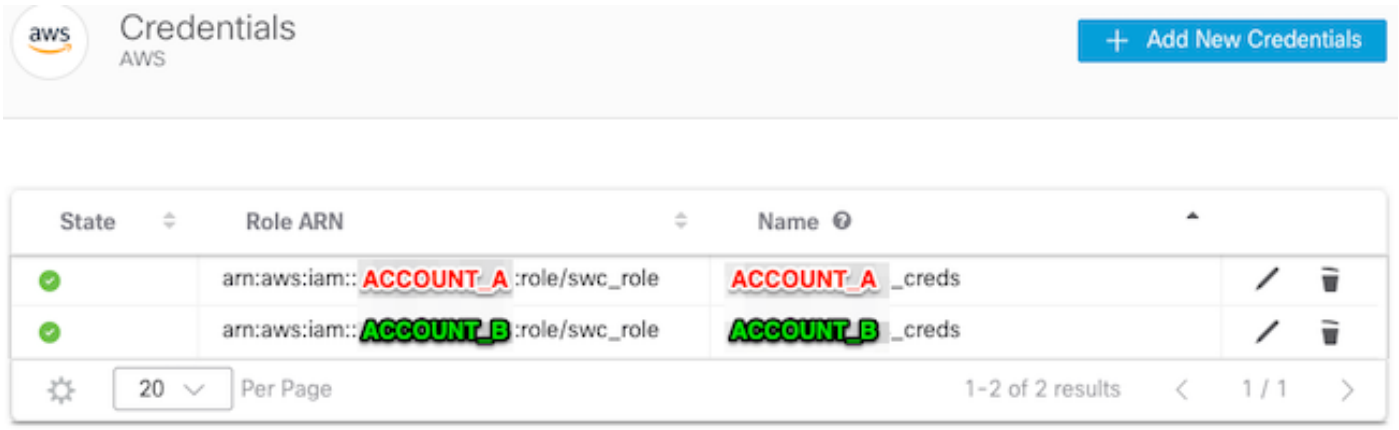
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Sua página de logs de fluxo do VPC na página da Web do Secure Cloud Analytics será semelhante a essa imagem após cerca de uma hora. URL para a página de logs de fluxo do VPC: **https://portal-name.obsrvbl.com/v2/#/settings/integrations/aws/vpc_logs**



Sua página Credenciais do AWS é semelhante a esta:



Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Se você não vir os mesmos resultados na página Log de fluxo do VPC, será necessário habilitar o Log de acesso do servidor do AWS S3.

Exemplos de registro de acesso ao servidor S3 (dados GET-ing do sensor SCA do S3):

acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000]

10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQPM6SB0YZNWE03 REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2FACCOUNT_B_ID%2Fvpcflowlogs%2F&encoding-type=url HTTP/1.1" 200 - 421 - 13 13 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - ghD4o28lk0G1X3A33qCtXIg4qDRfo4eN3uebyV+tdCBQ6tOHk5XvLHGwbd7/EKXdzX+6PQxLHys= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 - acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQTXPDG4G6MY2CR REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2F&encoding-type=url HTTP/1.1" 200 - 445 - 33 33 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - geCd2CjQUqwxYjVs0JUt+gyEuKw92p3iJt52qx0A+bOaWhjaiNI77OxGqmvFlJZpMT5GePh6i9Y= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 - acfb735656a2b1bbd16c05582b753d11a9306f3a8dc20a4b9edc8c999aef9dd2 S3_BUCKET_NAME [10/Apr/2022:22:55:12 +0000] 10.0.129.197 arn:aws:sts::ACCOUNT_A_ID:assumed-role/swc_role/b401ed3c-58d1-472d-ab20-4801d0a7 CSQVVKEPV0XD9987 REST.GET.BUCKET - "GET /?list-type=2&delimiter=%2F&prefix=AWSLogs%2FACCOUNT_A_ID%2Fvpcflowlogs%2F&encoding-type=url HTTP/1.1" 200 - 421 - 11 11 "-" "Boto3/1.17.85 Python/3.6.9 Linux/5.4.0-1064-aws Botocore/1.20.85" - hHR2+J5engOwp/Bi7Twn5ShsDXNYnH5rcB8YByFJP5OnZb64S1Y7/d+c7BSbBb861TpuJ0Jtpes= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader S3_BUCKET_NAME.s3.amazonaws.com TLSv1.2 -

Referência do campo de log:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.